EURECOM Sophia Antipolis

Quarkslab

One for all and all for WHAD: wireless shenanigans made easy !

Romain Cayre, Damien Cauquil

DEFCON ENGAGE

Who are we ?

Romain Cayre, EURECOM

- maintainer of *Mirage*, a popular wireless swiss-army tool
- loves *cross-protocol attacks* (*Wazabee*)

Damien Cauquil, Quarkslab

- maintainer of *Btlejack*, a BLE swiss-army tool
- loves reversing stuff, including *embedded systems*

Introduction

Wireless tools are a mess

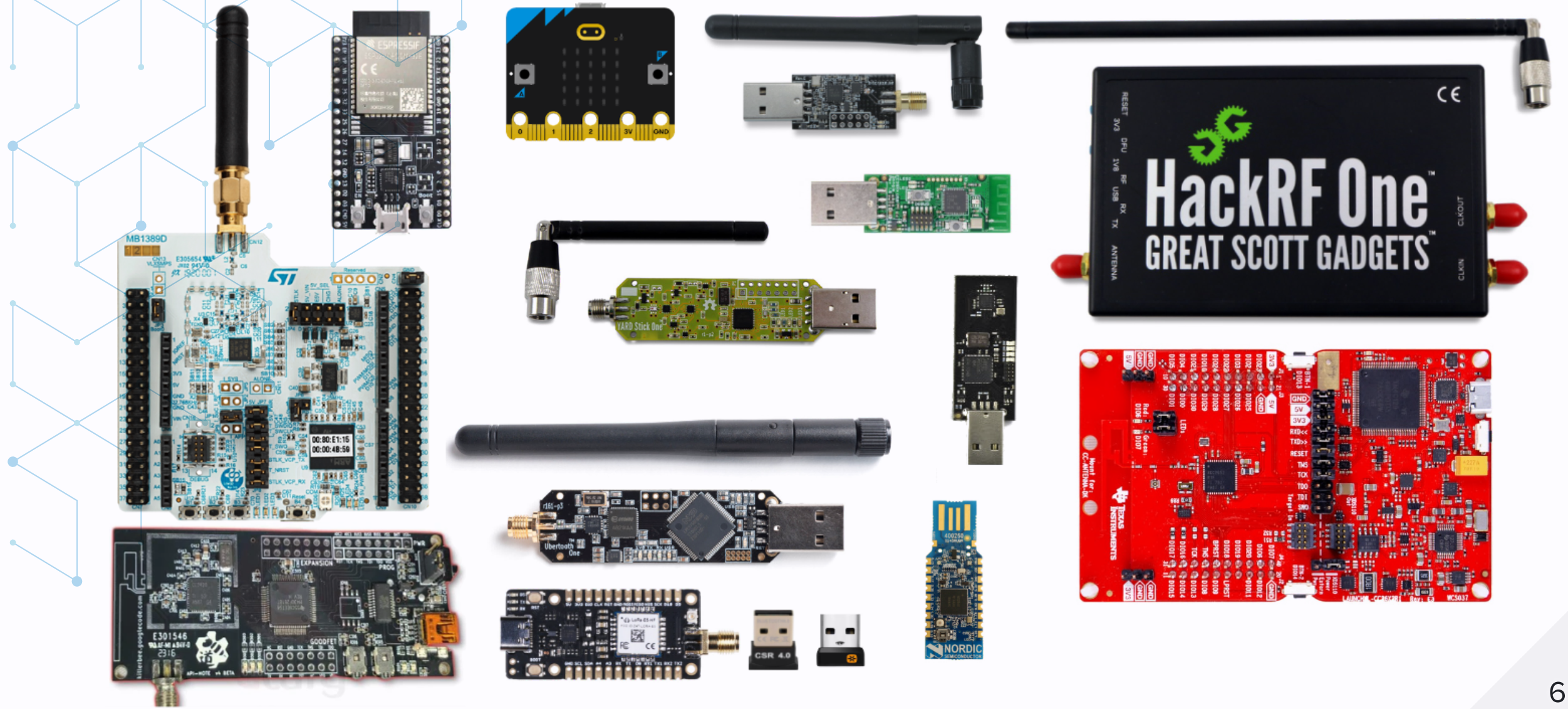
- **Different people** working on **different tools** and protocols
- Host/hardware communication protocols **not standardized**
- Everyone **reinvents the wheel** 🤔

Wireless tools are a mess

- **Bluetooth Low Energy**
  - *Btlejack* (BBC Micro:Bit)
  - *Mirage* (nRF52)
  - *Btlejuice/Gattacker* (BLE USB dongles)
  - *Sniffle* (TI CC26xx and CC13xx boards)

- **Logitech Unifying**
  - *Mousejack* (nRF24LU1, Logitech Unifying dongles)
  - *munifying* (Logitech Unifying dongles)
  - *Logitacker* (nRF52 Dongle)

Wireless tools are a mess



Consequences

- **Fragmentation**
  - Attacks/features **only work with a specific device**
  - We need to buy **a lot** of different hardware devices
  - **Need space** to store everything (**not travel-friendly**)
  - **Hardware discontinued** / Software deprecated

- **Waste of time**
  - Creating firmware and host/hardware protocol
  - **Facing and solving common issues**
  - **Difficult to modify/improve** a tool

How to solve this fragmentation problem ?

Fighting fragmentation

- **Extensible host/device communication protocol**
  - Supports multiple **wireless protocols** and PHYs
  - Open-source and extensible

- **Common libraries/framework**
  - Basic ready-to-use features for different platforms
  - Available for host and firmware

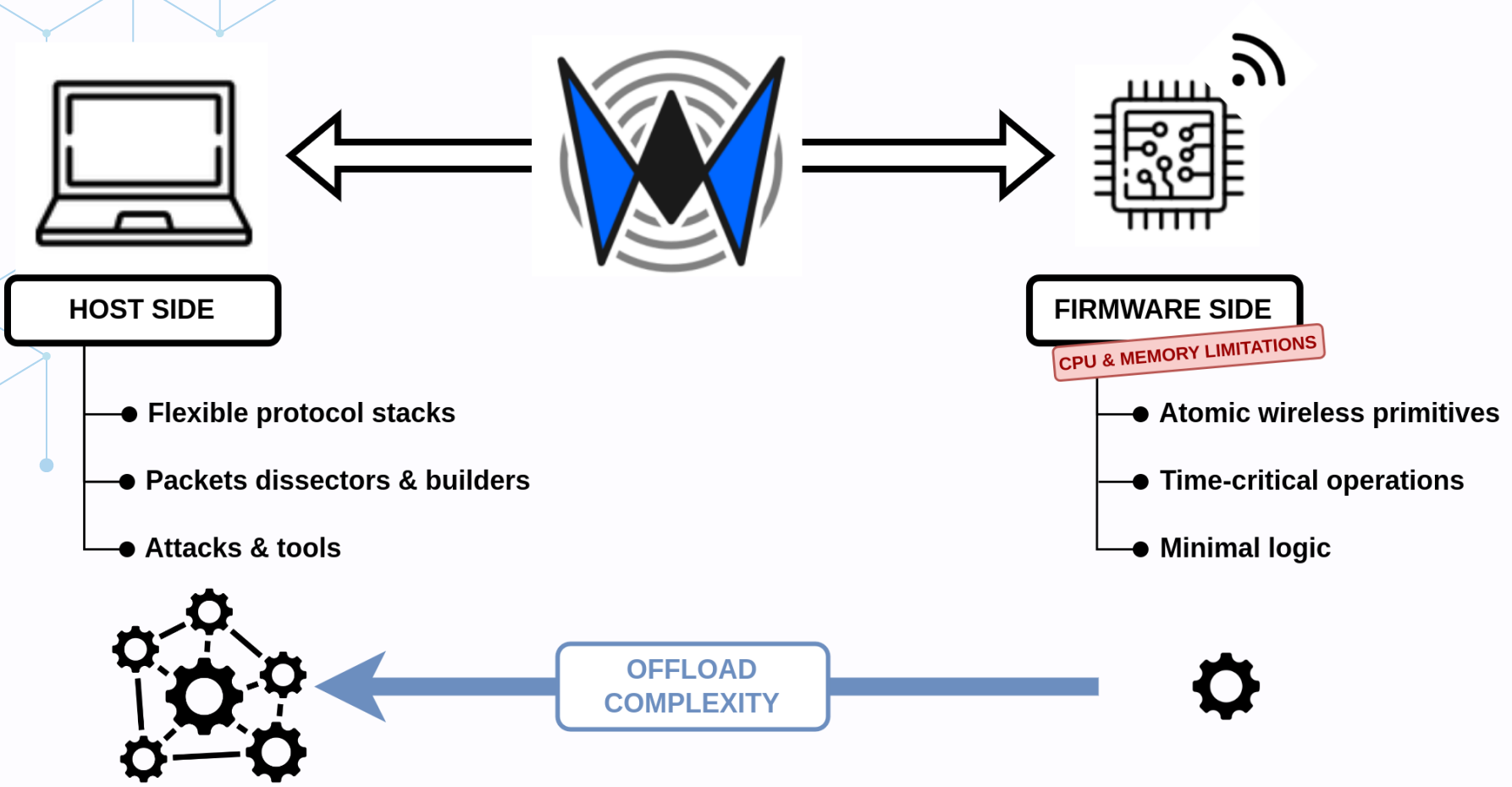
Fighting fragmentation

- **Encourage inter-operability & collaboration**
  - Everything is open-source
  - Heavily documented (usage and design)

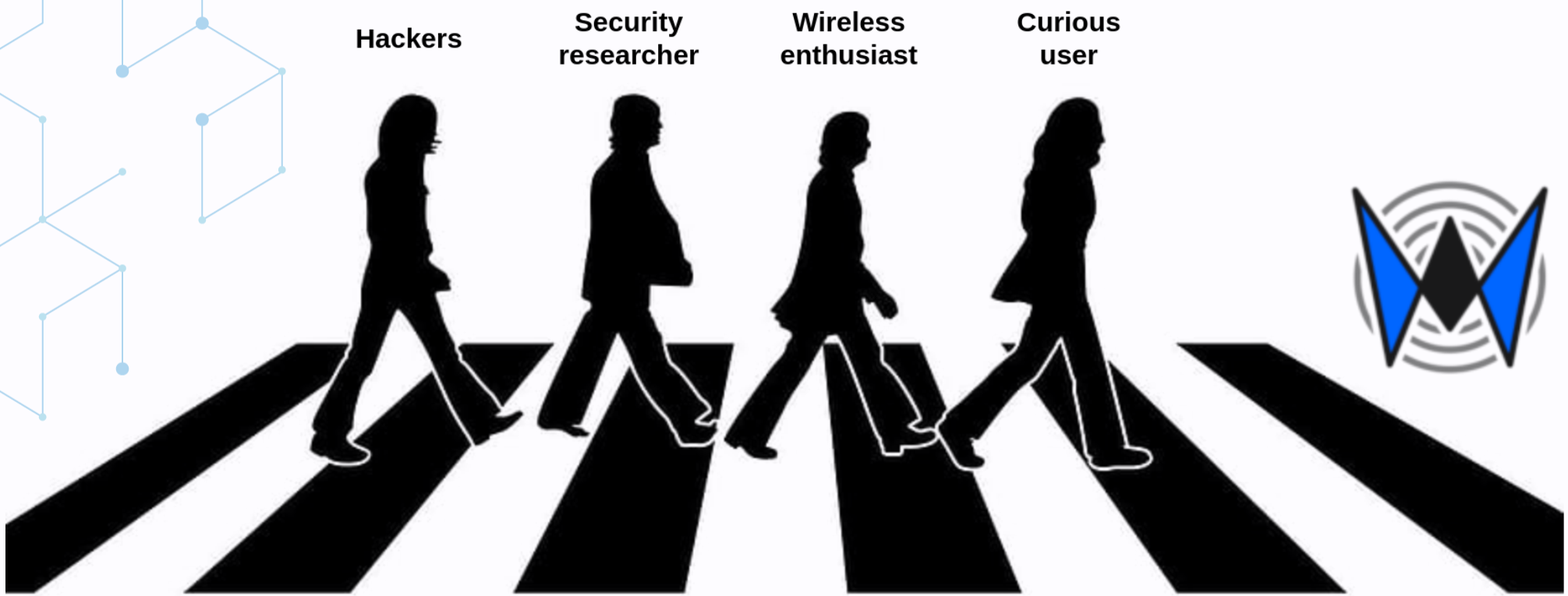
One protocol to rule them all!

- **Standardized**: properly defined protocol
- **Generic**: covers existing wireless capabilities
- **Modular**: multiple wireless protocols support
- **Evolutive**: designed to be extended & improved
- **User-friendly**: comes with C, C++ & Python parsing libraries

Let hardware do hardware stuff



WHAD is for everyone



EURECOM Sophia Antipolis

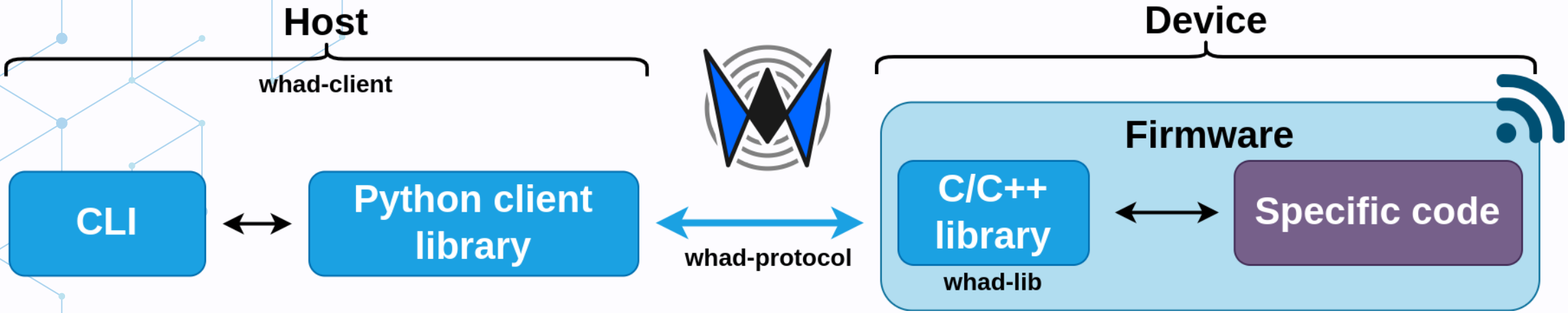
Quarkslab

What is WHAD ?

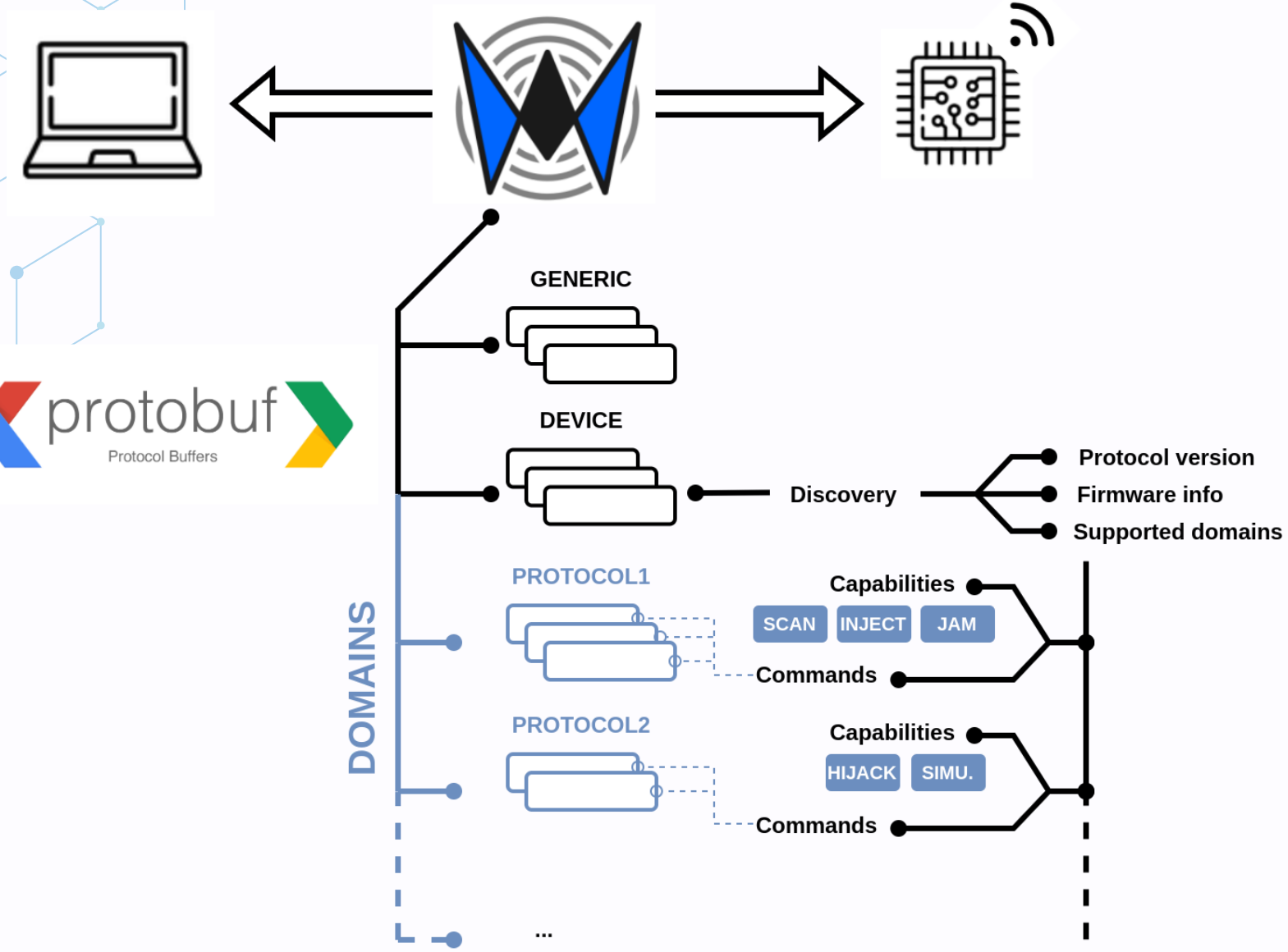
WHAD ?


Wireless
HAcking
Devices
Wireless
HAcking
for Dummies
imgflip.com

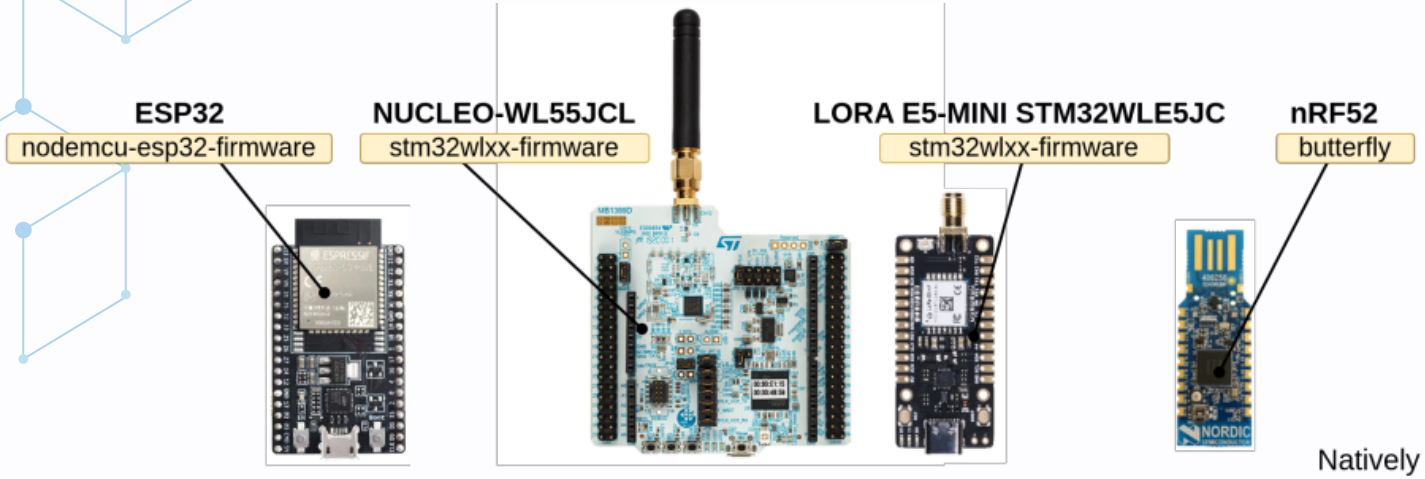
It's wayyyy more than a protocol!



Device discovery and capabilities

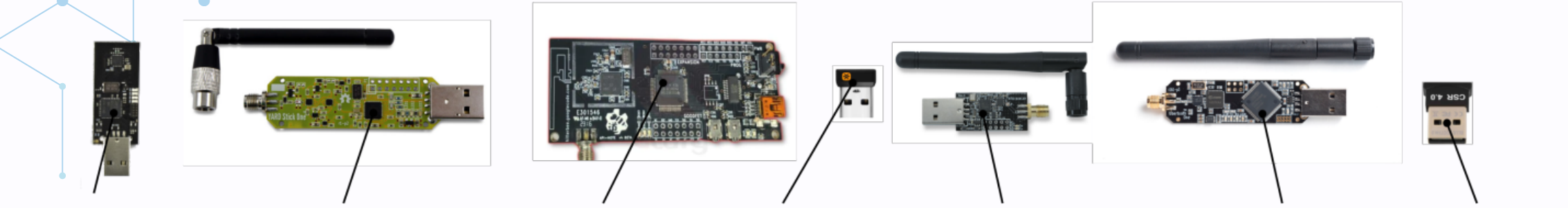


Compatible hardware



Natively supported by WHAD (whad-protocol)

Supported by WHAD (adaptation layer)



Supported wireless protocols

- WHAD *domains*: **PHY**, **BLE**, **802.15.4**, **ESB**, **Logitech Unifying**
- **PHY** supports various modulations:
  - **FSK/GFSK/MSK**, **ASK**, **LoRa**, **QPSK**
- Protocols based on some *domains* and **PHY**:
  - **BLE**
  - **ZigBee**
  - **RF4CE**
  - **LoRaWAN**

Extra capabilities unlocked

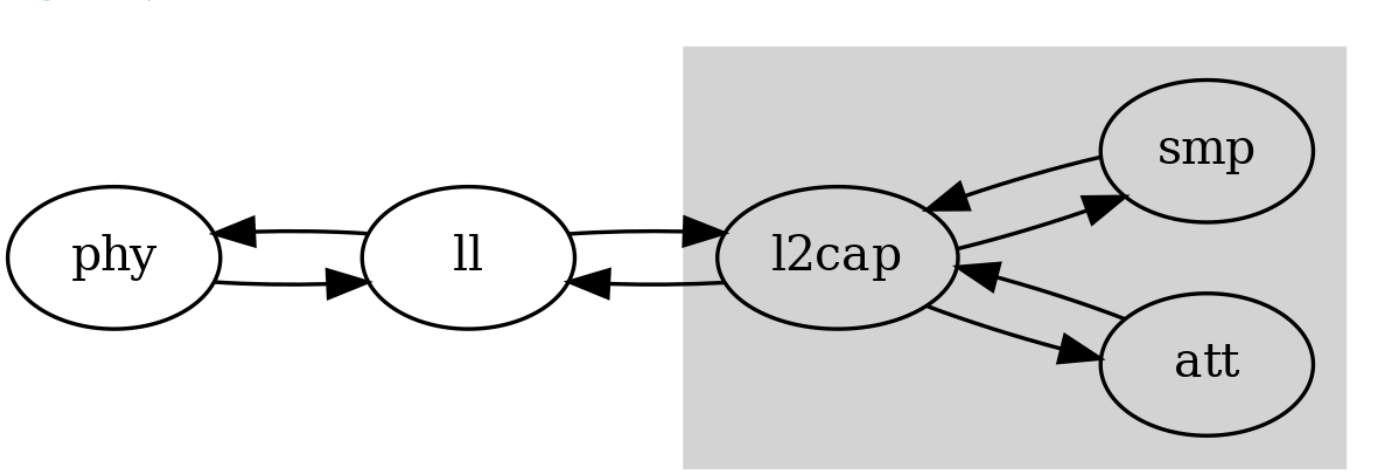
- **nRF52** firmware offers **ZigBee** support
  - Research paper WazaBee
    (R. Cayre, IEEE/IFIP DSN 2021)

- **ESP32 NodeMCU** supports raw BLE sniffing and injection
  - Research paper ESPwn32
    (R.Cayre, D. Cauquil, WOOT 2023)

Adding new protocols

- **WHAD is extensible**
  - WHAD has a **defined set of supported protocols**
  - Protocol is versionned
  - **Contribute** to WHAD to add new protocols! 😊

Our own stacks for better flexibility



- **Flexible stack model**
  - **Easy to modify** the behavior of a specific layer
  - Protocol stack state **snapshot/reload** 😎
  - **Unit tests** are easy to implement

Our own stacks for better flexibility

- We provide our **own protocol stacks** (full-python):
  - **BLE**
  - **Logitech Unifying**
  - **Enhanced ShockBurst**
  - **ZigBee**
  - **RF4CE**
  - **LoRaWAN**

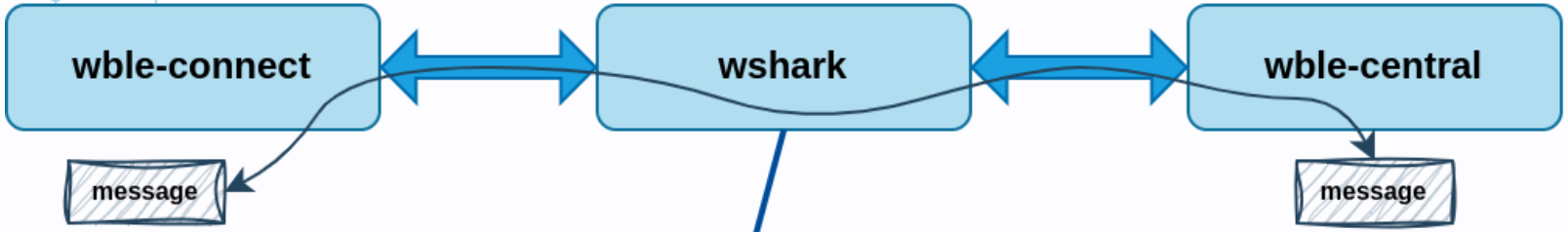
We love KISS

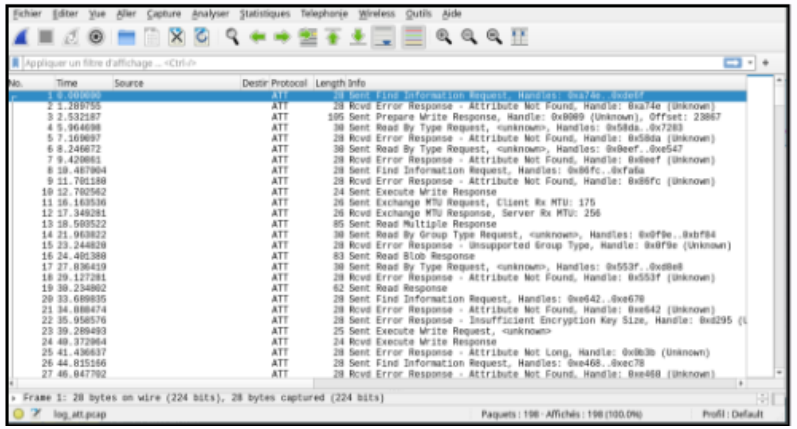
- **WHAD** provides a set of **simple command-line tools**
- Tools can be **chained** to create more complex tools
- **WHAD** also provides some **full-featured tools**
  - easier to use for new-comers
  - interactive and **allow exploration/reco**

We love KISS

EURECOM Sophia Antipolis Quarkslab

```
$ wble-connect -i hci0 00:11:22:33:44:55 | wshark | wble-central profile
```



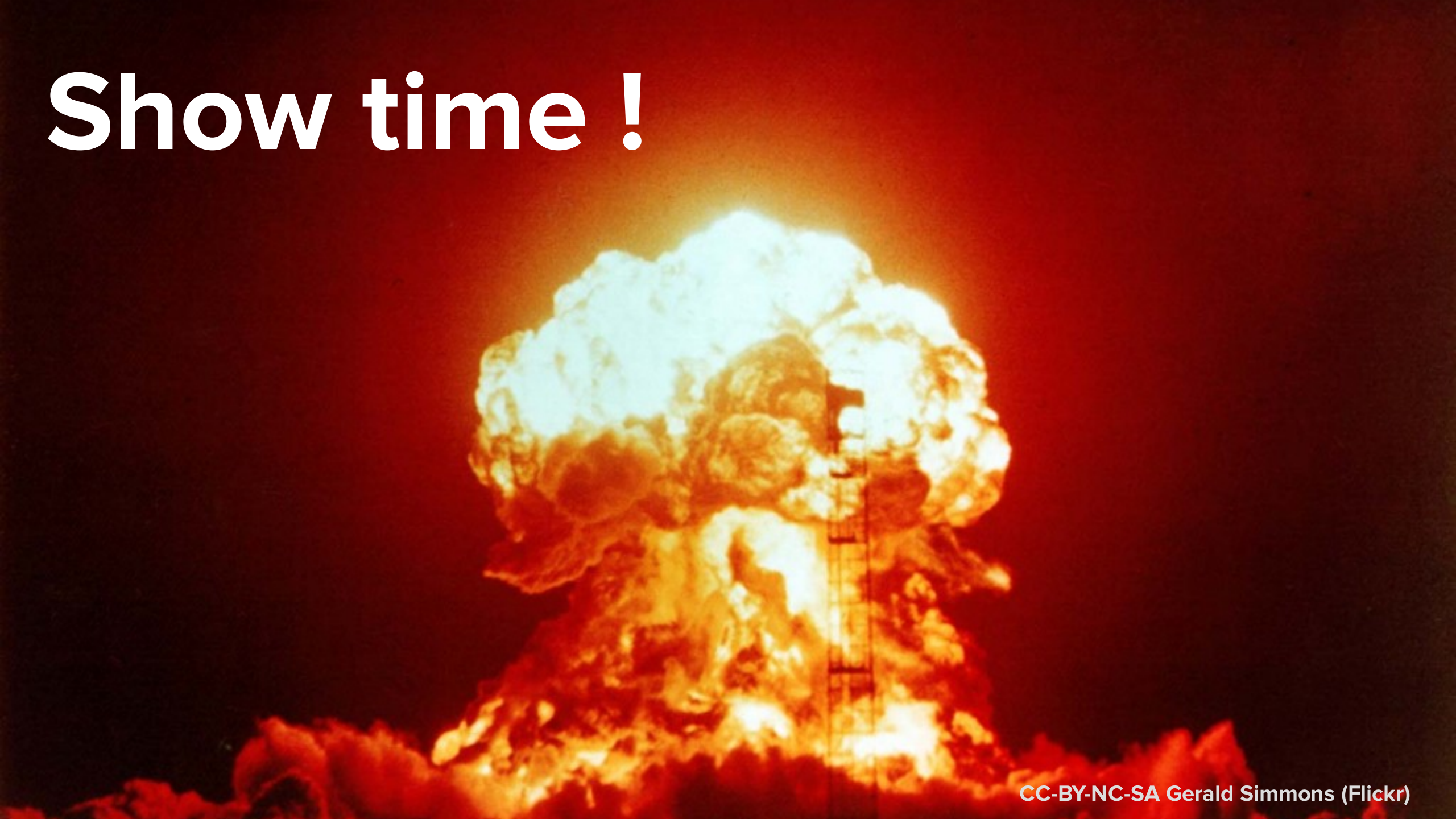


We love KISS

- **Unified common options** across WHAD tools
  - interface specification, logging, display options

- WHAD **provides wrappers** to create CLI applications 🥳
  - automatically identify and initialize WHAD devices
  - handle generic errors
  - **integrated interactive shell** and commands

Show time !



CC-BY-NC-SA Gerald Simmons (Flickr)

Exploring BLE devices (demo)

- Using WHAD's BLE interactive client **wble-central**
  - **scan** devices and get detailed info
  - **connect** to a target device
  - **enumerate** services and characteristics
  - **read/write** characteristics
  - **subscribe** for notifications

👉 demo1-ble-scan-connect.mp4

Exploring ZigBee network (demo)

- Using WHAD's ZigBee interactive client **zigbee-end-device**
  - **detect** any available ZigBee network
  - **join** a specific network
  - **enumerate** devices on this network
  - **control** any device

👉 demo2-zigbee-network-explore.mp4

Sniff and capture data (demo)

- **wsniff** is a multi-protocol sniffing tool
  - different output formats (**hexdump**, **scapy packet**, ...)
  - works with **any supported protocol**
  - able to **save data in PCAP** file

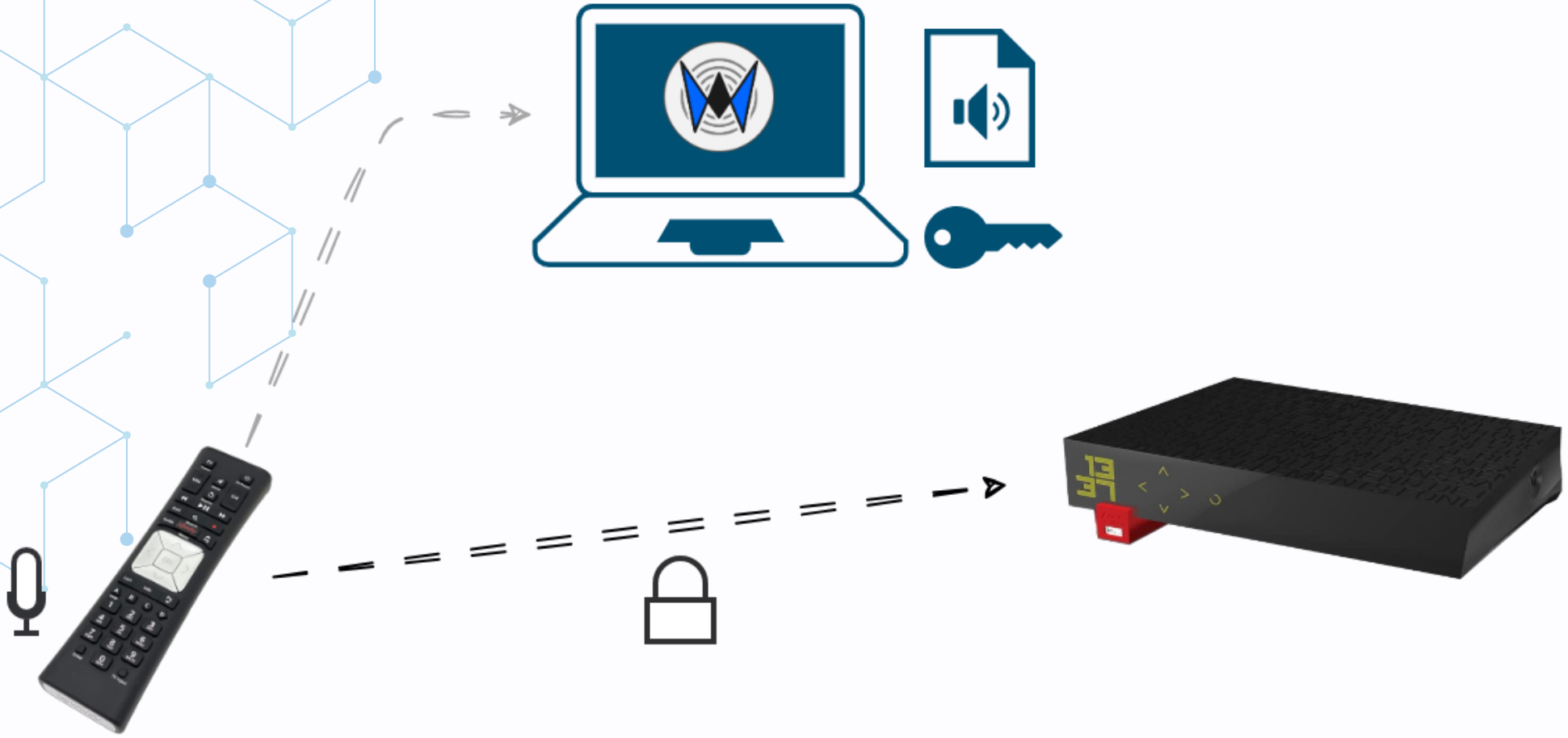
👉 demo3-whad-sniff.mp4

Sniff and process data (demo)

- **wsniff** can also be chained with other tools
  - allows packet features extraction (**wextract**)
  - packet dump processing through external tool

👉 demo4-whad-extract.mp4

Sniff RF4CE communication (demo)



👉 demo5-rf4ce-sniffing.mp4

Sniff traffic with wireshark (demo)

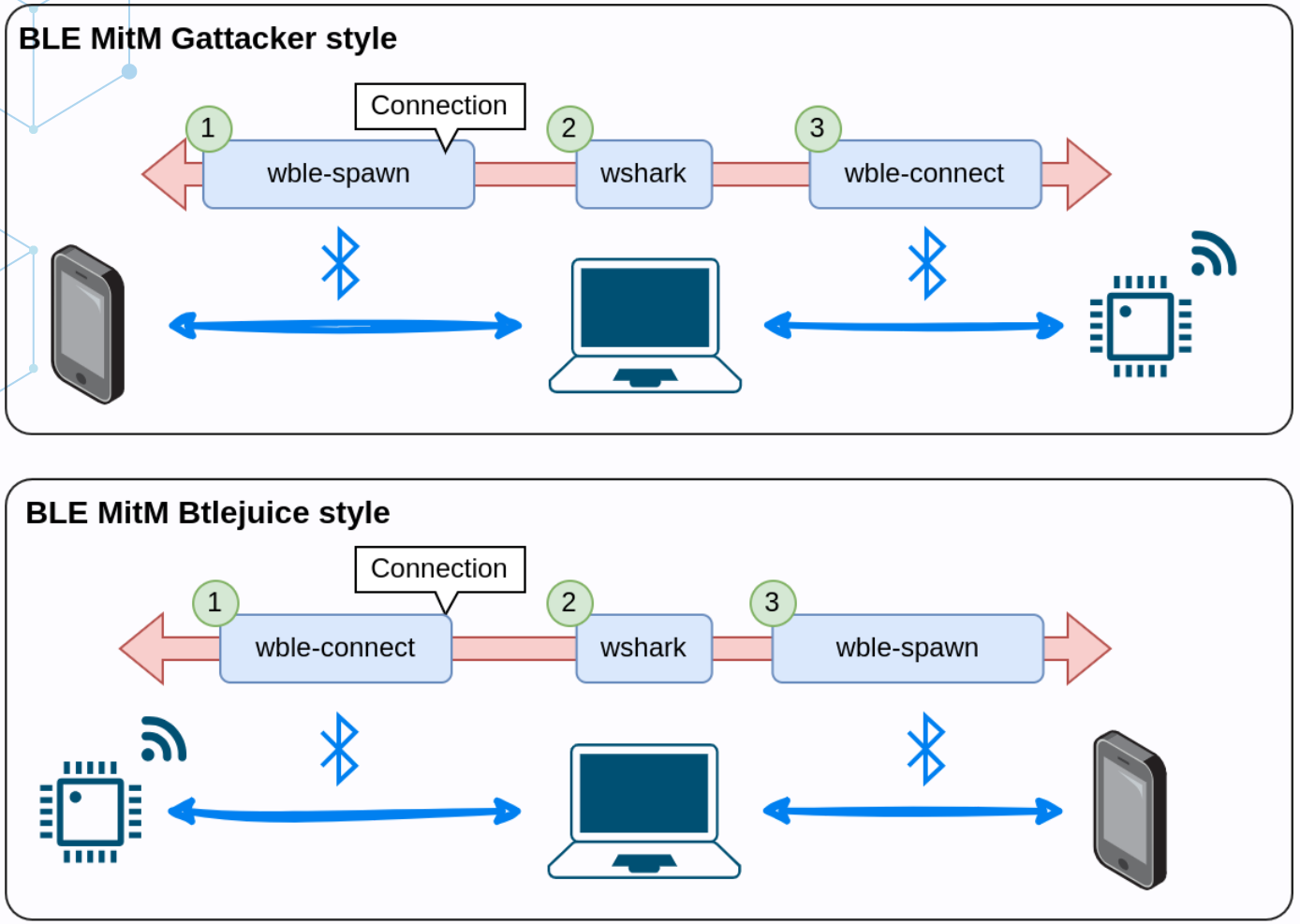
EURECOM Sophia Antipolis Quarkslab

```
$ wble-connect -i hci1 00:11:22:33:44:55 | wshark | wble-central profile
```

- **wshark** placed in a tool chain will **dump and show packets**
- act as a **packet proxy** in the chain
- **extra protocols** supported via **custom LUA dissectors**

👉 demo6-ble-sniffing.mp4

BLE Man-in-the-Middle (demo)



👉 demo7-ble-proxy.mp4

Emulate a BLE peripheral (demo)

- Using WHAD's BLE peripheral emulation tool **wble-periph**
  - **fully customizable** GATT profile
  - allows characteristic read/write/notification
  - useful for **quick tests**

👉 demo8-ble-periph.mp4

Implement a BLE peripheral (demo)

EURECOM Sophia Antipolis Quarkslab

```
class BatteryDevice(GenericProfile, BatteryService):
    """Device exposing a battery service"""

    @read(BatteryService.battery.level)
    def on_battery_level_read(self, offset, length):
        level = self.get_battery_level() - 10
        if level <= 0:
            level = 100
        self.set_battery_level(level)
        return self.battery.level.value

# Start advertising on hci1 with our BatteryDevice profile
periph = Peripheral(WhadDevice.create('hci1'), profile=BatteryDevice())
periph.enable_peripheral_mode(adv_data=AdvDataFieldList(
    AdvCompleteLocalName(b'BatteryDevice'),
    AdvFlagsField()
))
```

👉 demo9-ble-battery-device.mp4

LoRaWAN gateway (demo)

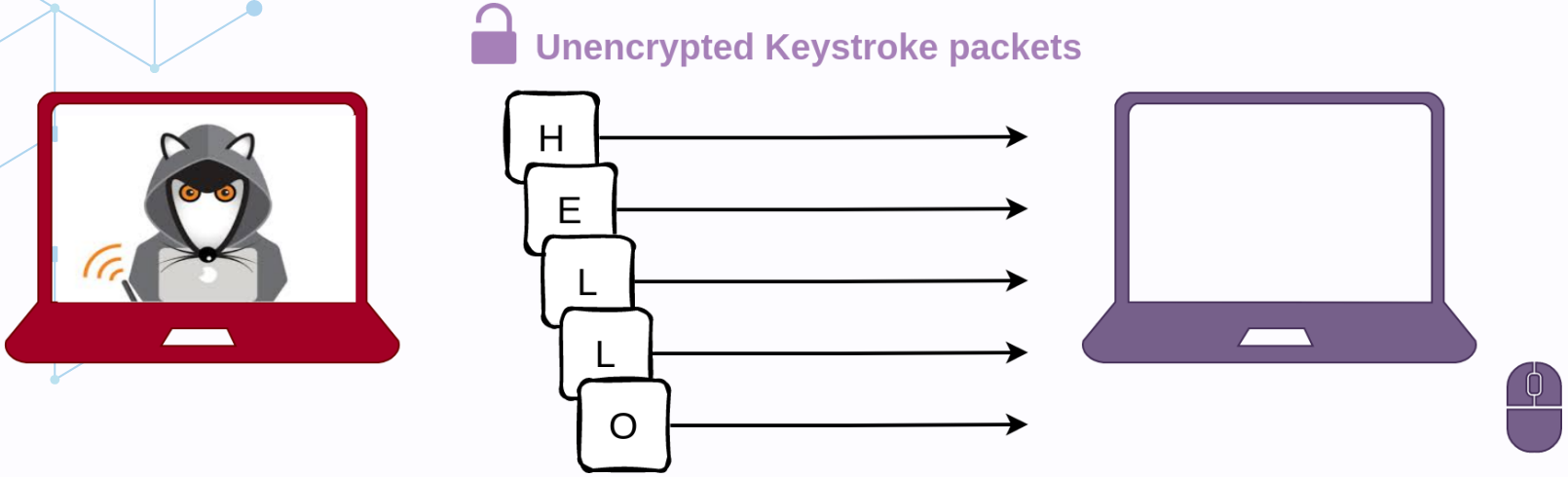
EURECOM Sophia Antipolis Quarkslab

```
class EchoApp(LWApplication):

    def __init__(self, devices):
        super().__init__(
            '51:75:61:72:6b:73:6c:61',
            '00000000000000000000000000000000',
            devices=devices
        )

    def on_data(self, node: LWNode, data: bytes) -> bytes:
        # Return the same data (echo)
        return data
```

- WHAD provides a **LoRaWAN** stack
- We set up a LoRaWAN **echo app** on an **emulated gateway**

👉 demo10-lorawan-gateway.mp4

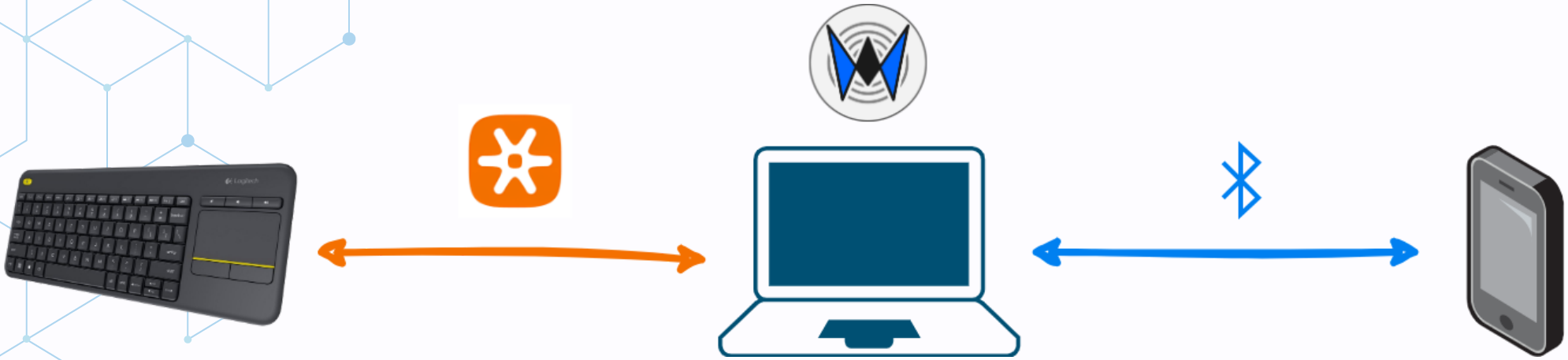
Emulate Unifying Keyboard (demo)



- **Scan** surrounding Unifying devices
- **Emulate a keyboard** to **inject unencrypted keystrokes** (MouseJack)

👉 demo11-logitech-unifying.mp4

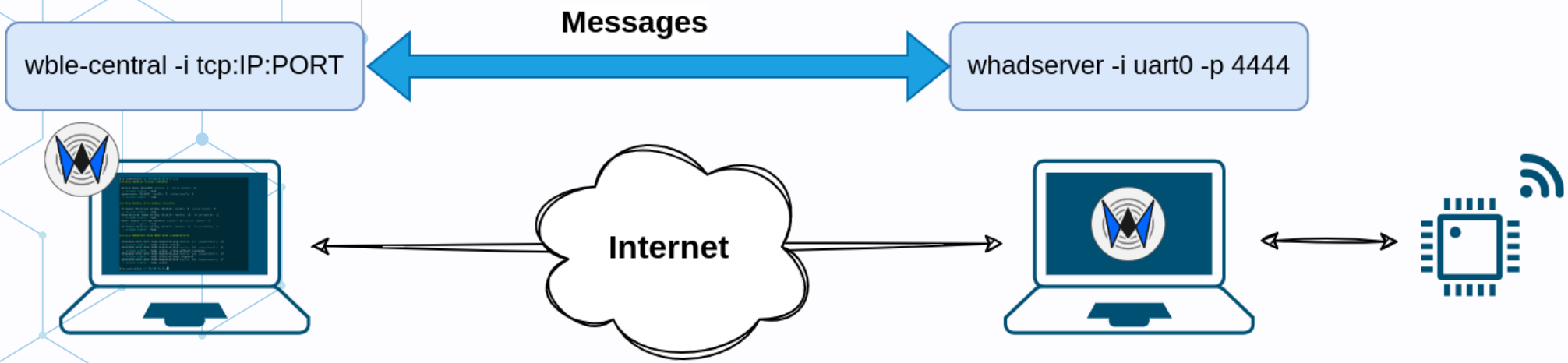
Cross-protocol bridge (demo)



- Turn a **Logitech wireless** keyboard into a **BLE keyboard**
- **Real-time** protocol conversion 🤩

👉 demo12-cross-protocol.mp4

Packets over the wire (demo)



- **whadserver** exposes a WHAD device **over TCP**
- **any tool can connect** to a WHAD TCP server
- allow **relay attacks** (with some latency)

👉 demo14-packets-over-wire.mp4

Hack all the things \o/

- WHAD has been used during last year by researchers
  - BLE GATT fuzzing project at Quarkslab (CVE-2024-24746)
  - Instrumentation of BLE protocol for Screaming Channels attacks

- Heavily used in **Hardware CTF** at Hardwear.io
  - BLE challenges are **100% emulated with WHAD**
  - LoRaWAN gateway also fully emulated

Conclusion

Public release (code & doc)

EURECOM Sophia Antipolis Quarkslab

```
$ pip install whad
```

- Documentation available on **ReadTheDocs**
- **Firmware files** available in sub-repos
- Code available on Github

Call for contributors

EURECOM Sophia Antipolis Quarkslab

- **Create compatible firmwares** for unsupported hardware
- **Report bugs** and issues on GitHub
- Help writing **documentation**
- Add support for **more protocols** !
- **Spread the word** and tell everyone to use it 

Last words

- **2 years of hard work** and we only scratched the surface of what WHAD is capable of
- Many researchers tried WHAD and helped:
  jduck, **Mike Ryan**, **Xeno Kovah**, **Slawomir Jasek**, **Jiska Klassen**, **Axelle Apvrille**, **MadSquirrels**, **Fenrisfulsur** 🙏

EURECOM Sophia Antipolis

Quarkslab

Q/A time

EURECOM Sophia Antipolis

Quarkslab

Thank you !